33 In part II, below, we identify the interests we seek to protect and explain why we find they are "substantial" interests to which commercial speech interests may be required to yield. Our conclusions are based on our view of the pertinent law. They are supported by comments we received from consumers in response to the Qwest opt-our notice, on comments received from stakeholders in this rulemaking, and on privacy values related to telephonic communications that are expressed in the statutory and constitutional law of our state.

34 In part III, below, we explain how our rules directly and materially advance protected privacy and free speech and association interests and why the means we have chosen are carefully crafted to impinge on any freedoms no more extensively than necessary. We weigh the relative merits of "opt-in'' and "opt-out" privacy protections by considering information in comments, including polling data and expert analysis related to consumers' experience with opt-out privacy notices in other industries, as well as consumer and stakrholdrr comments related to Qwest's recent opt-our notice.

35 While we are cognizant of telecommunications companies' commercial free speech interests, we weigh these interests against very important constitutional values on the customer's side of the equation. One's ability to keep private those communications thar one chooses (and in which one has a reasonable expectation of privacy, supported by existing law) serves viral constitutional values of privacy and free speech and freedom of association. Perhaps it is obvious, but the telephone is used for *private communications* with *others.* Iris thus an instrument by which these important and protected interests are achieved. While we recognize that, at some point, an advance in customers' privacy interests may represent a diminution in companies' commercial speech rights, we cannot ignore that the converse is also true: an increase in commercial usage of customer's CPNI at some point represents a decrease in the protection of the customers' inrerests.

36 We have sought to develop rules that are consistent with the US. Constitution, with Section 222 and the FCC's rules interpreting that statute, and with our own state laws and constitution. While we respect the FCC's approach to this topic, we nonetheless make our own findings about the kinds of interests we seek to protect and the balance we find it necessary to strike between consumers' interests and companies' interests.

37 On the totality of thcsc considerations, we find that the FCC's rules leavc certain substantial privacy, free speech and free association interests inadequately protected in Washingron State. As the FCC anticipated and expressly allowed in its order, we conclude that the provisions of law we arc entitled and rcquircd to consider and the record bcforc us require us to provide safeguards more stringent than those required bv the FCC's rules.

11. MAINTAINING THE STRICTEST CONFIDENTIALITY OF *AN* INDIVIDUAL'S COMMUNICATIONS OVER THE TELEPHONE IS A SUBSTANTIAL STATE INTEREST.

A. Because of the nature of services they provide, telecommunications companies are necessarily engaged in full-time monitoring of private communications.

38 As the owners and operators of telecommunications lines, telecommunications companies might be said *to* be engaged in full-time "wiretapping" of the phones or equipment that connect to their lines." The wiretapping laws plainly extend to carriers insofar as carriers might attempt to listen in on phone calls or otherwise intercepr the content of what they carry. Aut additional personal information is acquired in setting up calls and billing for them. As we will discuss below, the wiretapping laws cannot include any blanket prohibition on the acquisition, storage, and use of such information, because it is not possible to run a phone network without it.

39 Telecommunications carriers possess the capability to track certain information that results when subscribers use their telephones. Some of these tracking methods are commonly used (e.g., tracking long-distance calls for billing), while others may be used less frequently (e.g., tracking local dial-up calling to Internet service providers).

40 The technical capability of telecommunications companies to trace and track calling habits, and specifically to identify where and *to* whom the calls are being placed, has resided in the software of elecrronic network equipment for a

[12] *Huber, Kellog, and Thorne, Federal Telecommunications Law, §14.5.2,2d Ed.(1999).*

number of years. Although historically the primary use of the information companies collected was for forecasting growth and engineering the network to handle peak loads, recent federal legislation has required companies both to extend the types and amounts of information gathered, and to make this information available to government entities in certain situations.

41 With the passage of the Communications Assistance for Law Enforcement Act, or CALEA, in 1994, a telecommunications company is required to:

> [E]nsure that its equipment, facilities or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications, are capable of:
>
> (1) expeditiously isolating and enabling the government, pursuant to a court order, to intercept ...all wire and electronic communications carried by the carrier... land]
>
> (2) ...to access call identifying information...
>
> (A) before, during, or immediately after the transmission...

CALEA, Sec. 103 (a)

42 In Section 102 (2) of CALEA, "call identifying information" is defined as information from dialing or signaling that identifies "origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment."

43 Under the requirements of CALEA, a telecommunications company must at least have the capability to take the following actions:

- Track local calls
- Track long distance calls
- Track feature use
- Track answer or no answer
- Track three-way calling
- Track conference call participation
- Track 800 calls
- Track 900 calls

- Track length of local calls
- Track local dial-up Internet by ISP

For billing purposes, local service providers also record information regarding the length of long distance calls (regardless of long distance carrier) that originate and terminate on their switches. They may also track the number of rings before a phone is answered, either to start the billing of the long distance call, or in order to forward an unanswered call.

44 While a telecommunications company might not actually use **all** of this information on a day-to-day basis, and might not even track a customer's usage regularly, the technical capability to collect the information is certainly available. Without certain restrictions, the companies potentially could use the information for marketing or other purposes.

B. The development of a marketing database industry has turned private information in the possession of any business, including telecommunications companies, into a potential source of revenue.

45 Many believe, with good reason, that we are lately experiencing an erosion of our private sphere — not at the hands of government, but at the hands of private enrerprise. Advances in information technology and the search for improved efficiencies in productivity, which we herald in other contexts, arc driving the trend.[13] As stated in a research paper prepared under auspices of the Washington State Attorney General and the University of Washington School of Law:

> The information revolution, the affiliation of previously unrelated types of businesses, as well as the growth of data mining[14] and

---

13 Scholars have foreseen the threat that database technology poses to personal privacy for some lime. "[M]any people have voiced concern that the computer. with its insatiable appetite for information, its image of infallibility. and its inability to forget anything that has been stored in it. may become the heart of a surveillance system that will turn society into a transparent world in which our homes, our finances. and our associations will be bared to a wide range of casual observers. including the morbidly curious and the maliciously or commercially intrusive." A. Miller. *The Assault on Privacy: Computers, Dora Banks, and Dossiers 3 (1971).*

14 A standard definition for data mining is the non-trivial extraction ofimplicit. previously unknown. and potentially useful knowledge from data. Another definition is that data mining is a variety of techniques

> target marketing have contributed to a change in data collection. A consumer's personal information has the potential of being bought and sold like any other valuable commodity.
>
> * * *

46 There are currently more than one thousand companies compiling comprehensive databases about individual consumers, a ten-fold increase in just five years.[15] Rather than engaging in mass marketing, they focus on gathering as much information as possible about specific people to engage in targeted or "profile" marketing. By compiling layer upon layer of information about specific individuals, they are able to produce a profile based on income, lifestyle, and an enormous variety of other factors."[16]

> Using these databases, it is possible to identify people by what many would consider private aspects of their lives, including their medical conditions, their SAT scores, and their ethnicities.[17] Those selected by their personal characteristics can be targeted not only by direct marketers, but also by layers, insurance companies, financial institutions, and anyone else who has the funds to pay for the information.'"[18]

47 In short, there is an emerging market for information that may be used to predict individual consumers' receptiveness to offers of particular products and services. We are concerned that telecommunications companies, in their efforts to find new sources of revenue; may wish to sell or make other financial

---

used to identify nuggets of information or decision-making knowledge in bodies of data. and extracting these in such a way that they can be put to use in areas such as decision support, prediction. forecasting. and estimation. *See http://www.dacs.dtic.mil/databases/url/key.hts?keycode=222* (this explanation and citation is contained in the original research paper).

[15] *Mike Haich. Electronic Commerce in rhe 21st Century: rhe Privatization of Big Brother: Prorecring Sensitive Information from Commercial Interests in the 21st Century. 27 Wm.Mitchell L. Rev. 1457. 1471 (2001) citing Robert O'Harrow Jr., Daru Firms Getting Too Personal?, (Wash. Post) March 8. 1998 at A-1* (this citation is contained in the original research paper).

[16] *Id. at 1471* (citation is contained in the original research paper).

[17] *Id. ar 1471* (citation is contained in the original research paper).

[18] *Sellis, Ramasastry, Kim. and Smith, Consumer Privacy and Data Protection: Protecting Personal Information Through Conimercial Best Pracrices. pp. 9-10 (2002).*

use of records about customer communications. As described above, bccausc of the nature of the services they providc, telecommunications companies have a window on a large amount of very personal and potentially very telling information abour their customers. We find that it is therefore imperative to clarify, in the face of this potential source of revenue, rhat certain information about customers' communications patterns is off-limits to marketing use and disclosure to third parties, at least without the customers' express approval.

48 Finally, we observe that the readv commercial availability of call detail would make a mockery of protection of rhat same information from use by government: in the pursuit of compelling state interests such as the prevention and prosecution of crime, individual law cnforccmcnr agents and agencies of government could obtain the information nut only by presentation of a search warrant authorized by a judge bur also merely by purchasing it from rhc company or from any of a number of other commercial database suppliers.

C. The potential harm from use and disclosure, without consent, of individually identifiable call detail information is significant.

49 We embrace the FCC's objective of giving consumers a realistic opportunity to control the disclosure ofinformation about themselves tu parties outside of the telephone company. Rut to this we add a second objective of our own: that of curbing, even *within* the company, the creation of intrusive new profiles of individuals' communications patterns from what would otherwise be anonymous data. We explain both of these objectives in turn below.

1. *Without express consent, the disclosure of call detail could cause embarrassment, pecuniary loss, ora threat to safety.*

Fear ofdisclosure could chill citizens' use of the telephone to freely speak and associate with *others.*

50 Washingtonians have long relied on the assumption that records of whom they call and who calls them will be used only as necessary to provide the service to which they subscribe or to bill them for toll service. It is important *to* consider

the exact interests that would be harmed by the disclosure of this type of information, which we define as "call detail."

51 Justice Stewart, in a dissenting opinion to *Smith v. Maryland*, 442 U.S. 735, 748 (1979) stated this interest succinctly:

> Most private telephone subscribers may have their own numbers listed in a publicly distributed directory, but I doubt there are any who would be happy to have broadcast to the world a list of the local or long distance numbers they have called. This is not because such a list might in some sense be incriminating, but because it easily could reveal the identities of the persons and places called, and thus reveal the most intimate details of a person's life.

52 The specific kinds of potential harm of such disclosure are limitless, but a few examples are illustrative:

- People who wish to remain anonymous for their own safety—such as people who are subject to abuse or stalking or who might be sought for retaliation—could be endangered if it were possible for others to obtain lists of calls by or received by such person's relatives.

- People could be screened by prospective employers or fired from their jobs based on perfectly lawful communications with people or organizations to which their prospecuve or current employers object.

- Candidates for political office could face unfair scrutiny based on associations with organizations and people with whom telephone records indicate they or their family members have communicated.

- People wishing to intimidate or harass members of particular political causes, lifestyles or practices, or religions, could obtain organizations' calling records and with the help of a reverse telephone directory, determine the names and addresses of people connected with such causes, practices, religions, etc.

- Reporters could have sources compromised, despite assurances that the sources would remain anonymous.

- Firms could gain insights into their competitors' trade secrets such as the identity of suppliers, call volumes, and, with the aid of a reverse directory, the identity of a competitor's customers.

- With data about answered/unanswered calls, thieves could find out when an individual is likely or unlikely to be home.

53 Aside from these specific kinds of harm, there would also be a more generalized, but profound, harm to all of us, and to society. The ability of individuals to keep their personal communications private is a bedrock value, protected by our federal and state constitutions in several ways. Privacy interests are protected, as are free speech and association interests. Private free speech and association might be said to be triply protected. The primary purpose of a phone, after all, is to communicate with another person. If citizens fear that their use of the telephone will result in disclosure of very personal information, they will be reluctant to *use* the telephone for its intended purpose: *speaking* to *others*.

54 The instances listed above are all examples of harm that could result from disclosure of private call detail outside the telecommunications company. Every party to this rulemaking appears to concede that protection from these kinds of harm represents a substantial interest.[19] Many telecommunications company commenters stated that they *do not* currently disclose individually identifiable CPNI, which includes what we define as call detail information, to third parties. None stated they do make such disclosures.

55 We conclude that these kinds of potential harm are grave enough that companies should not be allowed to assume consumer consent for disclosure of call detail to third parties without explicit "opt-in" approval from the customer.

---

[19] The court in *U.S. West* expressed some concern about the FCC's articulation of this interest, but ultimately assumed that the government had asserted a substantial interest in protecting people from the disclosure of such information. *182 F.3d at 1235-36.*

2. *Even within a company, call detail is too sensitive to be used for profiling or targeted marketing, withouta customer's express consent.*

56 The consumer interests discussed above could be protected, to some degree (chough in our view nor adequately[20]) by a rule that simply prohibits disclosure of call detail outside the company —— r perhaps more broadly, outside the "corporate family."

57 Even if it were possible, however, to dcvisc a reliable system to ensure that call detail information would not be used in a way that results in any of the types of harm mentioned above, but only to dcvclop profiles of individual consumers for direct marketing by the company that serves them, there would still be the potential for a serious and substantial invasion of privacy," with its consequent effects on other interests.

58 To be clear, our goal is not to curb marketing *per se.* W e accept the premise that as consumers, we benefit when producers, as a result of knowing something about prior purchases we have made, are better able to inform us of goods and services that might bc of use to us, thereby allowing us to make better-informed purchasing decisions. However, where some kinds of information are concerned, this benefit is outweighed by consumers' unwilling loss of control over what they wish to reveal about themselves and for what purposes.

59 One consumer advocate recently described the types of privacy invasions that could result in the absence of rules prohibiting access to call detail:

> A consumer desiring a phone number must give personal information to the phone company. Information thereafter is developed from the consumer's phone patterns, such as whether

---

[20] We are concerned that the risk of harmful disclosure we describe in the preceding section would increase if call detail information were permitted to tlow to additional company personnel or company agents or contractors for the purpose ofdeveloping profiles of individuals *for* targeted marketing purposes.

[21] By privacy, we mean the interest in controlling disclosures of private information about oneself. We do not use the word io refer to the interest in not being bothered in one's home by sales calls. Consumers have other legal tools at their disposal to deal with the latter kind of privacy invasion. *See* RCW *19.158.110(2),* which provides that if recipient of a telemarketing call indicates she does not want to be called again. the marketer must not call again for at least one year and may not sell or give the person's name and number to other marketers

> the individual makes calls during the workday or calls certain phone numbers, like pizza delivery, on certain days and times of the week. Certain repetitive calls, such as regular calls out-of-state, can give clues as to the location and behavior patterns of family members. The frequency and duration of telephone calls to health care or insurance providers can give important clues about a family's health concerns. An observer can run consumers' call patterns through computerized screens to find consumers with "desirable" behavior patterns. Only the observer's ethic will hmit the ends and means for using the information. More importantly, a company can secretly target the consumer without revealing how extensively these phone patterns made the consumer's personal life an open book."

60 A group of state attorneys general expressed similar concerns to the FCC in the wake of Qwest's issuance of its poorly received opt-out notice in January of 2002:

> While the carriers might not disclose this highly valuable information to their competitors, they would disclose this information to marketing partners for the purpose of jointly marketing products and services unrelated to the customers' current service selection and even unrelated to telecommunications services entirely. For instance, carriers could enter into joint marketing arrangements with providers of certain types of medical products, and send solicitations to the homes of customers who call certain types of doctors or other health care providers. Similarly, carriers could enter into contractual arrangements with telemarketers to sell the telemarketers the names of customers who call certain retailers, or who access the web for a certain period of time or at a certain time of day. The type of information that telemarketers and joint marketing partners would find useful, and therefore be willing to pay for, is limitless. Telemarketers would use this infinite variety of CPNI information in selecting targets for an infinite variety of

---

[22] *Letter* dared *May* 2Y. *2002 io the Utilities Division of the Arizona Corporation Commission from Lindy Funkouser,* Direcror *of Arizona's Residential Utility Consumer Office*, quoted at p. I5 of *Comments of Public Counsel, Attorney General of Washington* (May *22.2002)* in this proceeding.

> solicitations, and the carriers would generate new sources of income from this resource. The only party to the transaction that will not have consented, and will not necessarily benefit, is the customer.[23]

61 The FCC's rules attempt to address the threat of this kind of invasive monitoring. They do so by restricting the use of information that is obtained without express, opt-in customer approval to the marketing of *communications-related* services and they require companies to limit their affiliates, independent contractors, and joint venture partners to this use of CPNI by contract. *47 C.F.R. § 64.2007(b).* We choose, for the reasons stated above, to require opt-in approval for *any* use of call detail information. Also, as we will explain, we draw the definition of the corporate family (outside of which the company may not disclose a customer's CPNI without express approval) more narrowly.

62 The technology of telecommunications, and federally-mandated identification and preservation of calling information, give telephone companies access to more intimate information about their customers than most other businesses possess. Telecommunications companies are in a position similar to that of health care providers, insurance companies, some kinds of financial institutions, cable providers, and video stores, in that they are in a position to gain a window on sensitive information about individual customers.[24]

---

[23] *Letter dated December 21, 2001, from 39 Attorneys General, to Federal Communications Commission, In matter of Telecommunications Carrier's Use of Customer Proprietary Network Information, CC Docket No. 96-115 and 96-149.* For many years, Judge Greene invoked concerns about misuse of customer information as a reason to bar phone companies from providing online information services of any kind. Although Judge Green was concerned about competitive issues, his concerns also have a strong privacy dimension. Through "control of its customers' lines of communication," a local phone company would "also have access to their lines of credit, travel plans, credit card expenditures, medical information, and the like. On the basis of a subscriber's telephone calling patterns with respect to information, an RBOC [Regional Bell Operating Company] could easily pinpoint that subscriber for the sale of RBOC-generated information and the sale of other products and services connected therewith, to the point where that company would have a 'Big Brother' type relationship with all those residing in its region." *United States v. Western Elec. Co., 6763 F. Supp. 525, 567 n. 190 (D.D.C. 1987), rev'd in part, aff'd in part, 900 F.2d 283 (D.C. Cir. 1990); see also United States v. Western Elec. Col, 714 F. Supp. 1, 12 n. 40 (D.D.C. 1988) (Bell companies barred from offering "user profile" services).*

[24] Incumbent local exchange carriers ("ILECs")—the most outspoken opponents of rules requiring express customer approval for the use of private information—are different from these other kinds of businesses in a significant way: their customers do not, in most cases, have the ability to choose another provider who will respect their privacy wishes.

Lawmakers have acted in fields such as these,[25] to ensure the confidentiality of particularly sensitive information. As we will discuss below, lawmakers in this state have acted also in the field of telecommunications privacy.

63 Unlike the FCC, we are concerned that a significant privacy interest, recognized by our state law and within the reasonable expectations of Washington consumers, would be compromised by a rule allowing a telecommunications company to engage in data mining and profile-building of its customers' communications patterns, even if only for the company's own targeted marketing purposes. To provide some specific examples, we find that the following practices, described either as a hypothetical possibility or as a current practice by commenters in this rulemaking, are too invasive of customer privacy to allow unless the company first obtains express customer approval:

- Monitoring customers' hourly, daily, or weekly call volumes and calls answered/unanswered, for use as a tool in approaching the customers and selling particular services to help them better manage their telecommunications. *Qwest's April 72, 2002 comments at page 6.*

- Monitoring customers' called telephone numbers to identify customers who might be receptive to an optional toll plan that offers a flat rate for calls made to other customers of that company. *Verizon's May 22, 2002, comments at page 9.*

- Monitoring the monthly amount a customer spends calling a particular area code to develop a sales lead list of customers who might be receptive to a plan that has special rates for calls made to a particular area code. *Sprint's May 22, 2002 comments at page 2; WITA's May 17, 2002 comments at page 2.*

---

[25] *Cable Communications Policy Act of 1984 (47 USC §521 et seq., §611); Video Privacy Protection Act of 1988 (18 USC §2710, §2711). Privacy of Consumer Financial and Health Information. Chapter 284-04 WAC. Fair Credit Reporting Act (15 USC §1681 et seq.); See also, Gramm-Leach-Bliley Financial Modernization Act (15 U.S.C. § 6801); Electronic Communications Privacy Act of 1986 (18 USC §1367, § 2232. §2510 et seq., §2701 et seq., §3117, §3121 et seq.); Electronic Fund Transfer Act (15 USC § 1693); Communications Assistance for Law Enforcement Act of 1994 (47 USC §§1001-1-10; §1021; 18 USC §2522); Driver Privacy Protection Act of 1994, and as amended in 1999 (18 USC §§2721-2725); Family Education Rights and Privacy Act of 1974 (20 USC §1232g); Federal Privacy Act (5 USC §552a); Right to Financial Privacy Act of 1978 (12 USC §3401 ersey.).*

64 We find rhar these uses of call detail constitute a privacy invasion for which a company should be required to obtain express, opr-in customer consent. The creation of thcsc profiles without customer consent is, in itself, an invasion of privacy, even if the information never makes it into the hands of a third part!. We arc also concerned thar such practices increase the **risk** thar companies will unintentionally disclose very sensitive information to third parries rhrough dishonest company agents or employees, or through negligence.[26] In other words, parr of our objective is to allow customers to control the creation of new points of exposure to their privacy.

65 Also, as we havc earlier observed, if cusromcrs fear an invasion of privacy when they use the telephone, they arc less likely to use the telephone to speak to and associate with others. We do not want to adopr rules thar would chill these activities.

D. Under existing Washington law, it is well established that telecommunications companies hold telephone calling records for a limited purpose—to deliver service and to bill for it.

66 Under Washington statutes it is both a criminal offense'. and a basis for civil liability[28] for anyone to intercept or record privarc communications transmitted by telephone without obtaining the consent of **all** rhe parries to the communication prior to each such interception or recording.'" Washington's

---

[26] Our record includes numerous complaints that opt-out directives to Qwest in January and February of this year were not recorded by company staff At issue was protecting customer information from disclosure to third patties, according to Qwest's opt-out notice. "when it is commercially reasonable to **do** so."

[27] Under RCW 9.73.080, anyone who violates RCW 9.73.030 is guilty of a gross misdemeanor.

[28] RCW *9.73.060* provides: "Any person who. directly or by means of a detective agency or any other agenr, violates the provisions ofthis chapter shall be subject to legal action for damages. to be brought by any other person claiming that a violalion ofthis statute has injured his business, his person, or his reputation. A person so injured shall be entitled to actual damages, including mental pain and suffering endured by him on account of violation of the provisions ofthis chapter. or liquidated damages computed at the rate of one hundred dollars a day for each day of violation. not to exceed one thousand dollars, and a reasonable attorney's fee and other costs of litigation."

[29] RCW 9.73.030 provides: "(1) Except as otherwise provided in this chapter. it shall be unlawful for any Individual. pannership, corporation. association. or the state of Washington. its agencies. and political subdivisions to intercept, or record any

> (a) Private communication transmitred by telephone, telegraph, radio, or other device between two or more individuals between points within or without the state by any

prohibition on violating a person's right to privacy is similar, but not identical to federal statutes pertaining to wiretapping of interstate and foreign communications.[30] Both Washington and Federal law plainly extend to phone companies,[31] particularly insofar as a company mighr attempt to listen in on phone calls or otherwise intercept the content of the calls they carry.[32]

67 As a matter of obvious necessity, however, there arc some broad exceptions under state and federal criminal statutes for the activities of telecommunications companies. Most importantly, Washington's statutory prohibition on intercepting or recording such communications docs not apply to:

> any activity in connection with services provided by a common carrier pursuant to its tariffs on file with the Washington utilities and transportation commission or the Federal Communication Commission and any activity of any officer, agent or employee of a common carrier who performs any act otherwise prohibited by this law in the construction, maintenance, repair and operations of the common carrier's communications services, facilities, or equipment or incident to the use of such services, facilities or equipment."

---

device electronic or otherwise designed to record and/or transmit said communication regardless how such device is powered or actuated, without first obtaining the consent of all the participants in the communication"

[30] *See 47 USC § 605(a)* ("no person receiving. assisting in receiving, transmitting. or assisting in transmitting. any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect. or meaning thereof, except through authorized channels . . .")

[31] For example, in *State v.* Riley. *121 Wn.2d 22 (1993)*, a criminal defendant alleged that US WEST had violated the statute by using a trace device to identify the number from which someone was repeatedly placing calls to the access number of a long distance provider in an apparent attempt to discover the access codes of the long distance provider's customers. US West gave the information to police and the police used it to obtain a search warrant. but the court analyzed whether *US WEST* had violated the law. The court found it had not because either (1) a tracer device does not intercept a "private communication" within the meaning of the act. or assuming it does (2) it was nonetheless permissible for the phone company to establish a line trap to trace hacking activity as part of its "operations" under RCW 9.73.070. The legislature later amended ch. 9.73 RCW to extend the protections of the statute to "the originating number of an instrument or device from which a wire or electronic communications was transmitted" — the information recorded by a trap and trace device like the one at issue in *Riley. RCW* Y. *73.260; 1998 Wash. Laws ch. 217, sec.* 1.

[32] *Hither. Kellogg, Thorne. Federal Telecommunications Law. 2nd Ed., § 14.5.2 (1999).*

[33] *RCW* Y. *73.070(1).*

68 An important way in which the federal wiretap law and Washington's privacy law differ is in how they treat information of the type contained in toll records. Federal courts have held that a phone company's disclosure of a customer's toll records, including numbers called and the length of the conversation (again, what our rule would label "call detail"), is not a violation of the federal wiretap statute." By contrast, as the Washington Supreme Court has stated:

> The State of Washington has a long history of extending strong protections to telephonic and other electronic communications. For example, RCW 9.73.010, which makes it a misdemeanor for anyone to wrongfully obtain knowledge of a telegraphic message, was enacted in 1909 and is based on section 2342 of the Code of 1881. The 1881 Code, adopted before statehood, extensively regulated rclegraphic communications. See Code of 1881, §§ 2342-62. Our present statute is broad, detailed and extends considerably greater protections to our citizens in this regard than do comparable federal statutes and rulings thereon.[35]

69 Under Washington statutes, the kind of "communications" that are not to be intercepted include not just the content of the conversation between the parties, but also the simple act of dialing from one telephone number to another."[36]

70 RCW 9.73.260 specifically provides that a court order is required for any person to use a "pen register" (a device that identifies all outgoing local and long distance numbers dialed, whether the call is completed or not) or a "trap and trace device" (a device to record the number of an incoming call) on someone's phone Line, and only law enforcement officers may petition for such orders."[37]

---

[34] *See. e.g. U.S.v.* **Barrer.** *4Y2 F 2d 150 (9th Cir. 1973).*

[35] *State v. Gunwall, 106* **Wn 2d 54. 66.**

[36] **Private communication** under RCW 9.73 includes "the dialing from one **telephone number to another."** *State v. Riley.* ***121 Wn.2d 22. 34*** *(1993): State v. Gunwall,* **106 Wn.2d 54. 69 (1986).**

[37] **Again, telecommunications companies' equipment is necessarily exempted from the definition** of pen **register:**

> **such term does not include any device used by a provider or customer** of a **wire** or **electronic communication service for billing, or recording as an incident to billing. lor communications services provided by such provider or any device used by a provider or**

71 Unlike its federal counterpart, Washington's law does not specifically prohibit divulging or disclosing communications; it only prohibits intercepting or recording them. As noted above, to the extent phone companies intercept or record such information in connection with the delivery of telecommunications services, the law does not apply to them. It could plausibly be argued that because there is no specific prohibition on *disclosing* such records, it would not be unlawful for the phone company to *use*, for any purpose that is not otherwise prohibited, call detail information that it has already recorded in the ordinary course of providing telecommunications services. We find that such an interpretation would be contrary to the privacy interests our legislature sought to protect in enacting laws to protect the privacy of telephonic communications. Part of our intention in adopting these rules is to fill the gaps between Washington's statutory protections on the privacy of communications and the FCC's CPNI framework.

72 Article I, Sec. 7, of the Washington Constitution[38] prohibits intrusions of privacy by the government of the sort that our rule prohibits for telephone companies. The Washington Supreme Court has held that the government may not obtain toll records and may not use a pen register without valid legal process such as a search warrant issued on probable cause. In so holding, the Washington Supreme Court quoted, as part of its reasoning, the words of the Colorado Supreme Court in finding a similar right to privacy:

> A telephone subscriber . . . has an actual expectation that the dialing of telephone numbers from a home telephone will be free from governmental intrusion. A telephone is a necessary component of modern life. It is a personal and business necessity indispensable to one's ability to effectively communicate in today's complex society. When a telephone call is made, it is as if two people are having a conversation in the privacy of the home or office, locations entitled to protection under . . . the Colorado

---

customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business.

RCW 9.73.260(1)(d). What is noteworthy about this exemption, like the more general exemption discussed above, is that it is not a blanket exception for phone companies, but an exception the companies are allowed for a limited purpose—specifically, billing and accounting.

[38] *Article I, Sec. 7, Wash. Const.* reads as follows: "Invasion of private affairs or home prohibited. No person shall be disturbed in his private affairs, or his home invaded, without authority of law."

> Constitution. The concomitant disclosure to rhc telephonc company, for internal business purposes, of rhc numbers dialed by the telephone subscriber docs not alter the caller's expectation of privacy and transpose it into an assumed risk of disclosure to the government."

73 To be clear, we recognize that search and seizure law is concerned with intrusions of privacy by the government—not by private enterprise. We nonetheless find the courts' analyses and holdings in these cases to be relevant to our analysis. In determining the extent of the Fourth Amendment's protection against warrantless searches, and the Washington Constitution's prohibition against being disturbed in one's private affairs, courts have been called upon to dcfinc thc sphcrc within which a citizen has a "reasonable cxpcctation of privacy." [40] We find this "reasonable expectation of privacy" inquiry to be much closer to the mark of what constitutes a substantial interest €orFirst Amendment purposes than the apparently more restrictive test posited in Qwest's comments. Qwest suggests that we have a substanrial interest (within the meaning of the *Central Hudson* test of regulatory burdens on commercial speech) only in protecting information thar, if disclosed, would be "highly offensive" to a reasonable person to whom it pertained. *Qwest comments of March 21, 2002, p. 11.* [41] Qwest notes that this is the standard for the tort of

---

[39] *State v. Gunwall, 106 Wn.2d 54.* 67 *(1986), citing People v. Sporleder.* 666 *P.2d 135. 141 (Colo. 1983).*

[40] See *Katz v. U.S , 389 U.S. 347 (1967).*

[41] Qwest also pointsout that this is the statutory standard for determining whether someone has a right to privacy in a particular piece of information. held by the government, that is sought for disclosure under Washington's Public Disclosure Act (PDA). ***RCW 42.17.250**, et seq.* The ***RCW 42.17.255*** standard for determining whether there is a right to privacy in information sought for disclosure is "ifdisclosure of information about the person: (1)would he highly offensive Io a reasonable person. and (2) is not of legitimate concern to the public." We find this too narrow a standard for our "substantial interest" analysis. The Public Records provisions ofthe PDA are suffused with the policy that citizens have a right to know what the governmental agencies they have created are doing. ***RCW 42.17.251***. This "government in the sunshine" policy is so important that the drafters ofthe citizen's initiative, Initiative *216,* chose to draw narrowly the individual's countervailing interest in the privacy of public records that pertain to himselfor herself. We note. however. that when the purpose ofa disclosure request under the PDA is merely commercial—as opposed to serving the central policy of open government — theprivacy protections of the Public Disclosure Act are far broader. **In fact, agencies are expressly not authorized to disclose lists of** individuals when such lists are requested for a commercial purpose. ***RCW*** 42.*17.260(9).* Moreover. the more specific disclosure exemptions/privacy protections of the PDA include information similar to what we seek to protect with our rules. *See e.g.* ***RCW 42.17.310 la)*** (Personal information in any files maintained for students in public schools, patients or clients of public institutions or public health agencies. or welfare recipients), *(l)* (Any library record, the primary purpose of which is to maintain control of library materials. or to gain access to informallon. which discloses or could he used to disclose the identity ofa library user).

invasion of privacy ("publicity given to private life") under the Restatement (Second) of Torts at 652D. We do nor read the 10th Circuit's decision as circumscribing the government's authority so narrowly as *to* allow us to place burdens only on company speech that would otherwise constitute a tort. A tort standard makes sense only when applied *to* the facts of a particular case.[42] Ton law is aimed at providing remedies for particular wrongs. Our rules necessarily have broader application because they are aimed at preserving customers' privacy and freedom of speech and association by reducing the risk of the occurrence of such wrongs.

E. Consumer comments following the Qwest opt-out notice reflect an expectation of privacy in telephone records.

74 During the course of this rulemaking, Qwest Corporation began sending opt-out notices to *ics* customers in Washington, as well as in the other thirteen states where iris the regional Bell operating company. Qwest's notices required customers *to* opt-out if they wished to prcvcnt use and disclosure of their personal account information, despite the opt-in requirements of Washington rules. Qwest's tactics were widely reported in the radio, television, and newspaper media, and many customers objected. Specific customer objections will be discussed below, but the general sendment of telecommunications customers was that personal account information should be protected unless the customer gives express permission for other uses. Customers also objected strenuously to the use of their private information by the telephone company itself to market other services to them.

75 The inescapable conclusion of the recent Qwest experience (consistent with the legal analysis of the preceding section) is that customers believe their telecommunications companies have a duty to protecr private information about them. Customers were astonished and angered at the notion that their

---

(nn) (The personally identifying Information of persons who acquire and use transit passes and other fare payment inedia including. *but* not limited *to,* stored value smart cards and magnetic strip cards].

[42] *See e.g., Hill v. MCI WorldCom, 141 F.Supp.2d 1205 (2001)* (Under Iowa law, telecommunications carrier's alleged disclosure of phone numbers and addresses of customer's friends to customer'sex-husband, who had previously stalked. threatened. and harassed customer. gave rise to claim for invasion of privacy based on the theory of publicizing private facts. where the facts disclosed would have been extremely embarrassing. highly offensive, and potentially dangerous Io a reasonable person in customer's situation. and the information disclosed was not of a legitimate concern to ex-husband).

telecommunications company might be able to disseminate information about them based on the assumption of their consent.

76 Beginning in mid-December 2001, Qwest mailed a bill insert to its customers, purportedly putting them on notice that the company intended to use and disclose CPNI for marketing purposes. Customers who objected to this use of their private account information were told to contact the company to opt out.

77 Customers who understood the company's intended use of their information objected strenuously and loudly. During January 2002, newspapers in this state published many letters from consumers who argued that Qwest was abusing its position as their provider of local telephone service and violating the customers' privacy rights. Newspaper editorials chastised Qwest for failing to respect its customers' privacy and exhorted regulators to act firmly to stop the intended practices." The WUTC received over 600 comments from customers. The customer response was extraordinary for the WUTC. To our knowledge, no policy issue has generated this many unsolicited comments from members of the public over any period of time, let alone in one month.[44]

78 Most of the customers who commented simply voiced their opposition to the Company's requirement that they opt out in order to avoid commercial use of their privare information. Others went further and made statements such as: "This is invasion of privacy and I thought it was illegal." Similar statements were made by nearly every commenter who went beyond "I am opposed to opt-out." However, some commenters went still further and commented on the nature of the relationship between them and their telecommunications company.

79 Those who commented about the relationship werr unanimous in what they said. With striking consistency, they stated that they view the relationship as a limited one in which they pay the company to provide telephone service and, to

---

[43] *See, e.g., Elizabeth Hovde, Phone Company Rings Customers' Bells: Will Qwest Ever Get the Voice Mail:'. The (Vancouver, Washington) Columbian, January 8, 2002: Editorial, Make "Opt Our" Easier for Qwest Consumers, The (Tacoma, Washington) News Tribune, January 9, 2002: Opinion, Qwest's Train Wreck. The Seattle Times, January IY. 2002.*

[44] The only instance in which customer comments erceeded these in the space of a month was during a strike by the Communications Workers of America against U S WEST. The strike lasted a month and tens of thousands of orders went unfilled. with the result that 750 people without dial tone contacted the WUTC to comnlain

rhc extent they must provide information to establish service or to complete a call (dial a number), they consider that the relationship docs not entitle the company to do anything with that information but use it to provide service.

80 Sonic examples of what people stated in e-mails to the WUTC:

- When 1 subscribe to any service, uhcrhcr it be the utility company, the gas company, or the phone company, I am providing information to thcm solely because they require it before they will provide a service to me.

- I need a telephone; therefore, 1 do business with Qwcst. I did not ever grant them permission *to* make money off of me, to solicit from me, to provide information about me to anyone for any reason.

- They are providmg us a service that we have contracted for. We are not here to provide them with unlimited information which THEY can sell to the highest bidder.

- We arc paying them for phone service. Our phone usage is our private business.

- The individuals supplied rhe information to the respective company for the singular purpose to contract a business relationship with that company. All information should be held private between the participants of that business relationship.

81 One comment spoke directly to the issue of non-disclosure in business relationships:

> My clients are major corporations. Every single one of them requires me to sign a non-disclosure statement prior to my even talking to them about how my services might help them. These non-disclosure statements also forbid me to discuss what the company is doing when using my services and what services I am providing them. If I did nor sign those non-disclosure agreements, 1 would not be able to get any work.

Clearly, customers do nor believe that their telecommunicarions company has, as an assumed or implied extension of the customers' purchase of scnicc, permission to use or disclose the cusromcrs' CPNI as the company pleases. Neither do customers believe it is enough, with respect to all possible uses and all types of CPNI, thar customers should only have notice and an opportunity to revoke such implied permission.

III. OUR RULE IS NARROWLY TAILORED TO PROTECT CONSUMERS PRIVACY AND FREE SPEECH *AND* ASSOCIATION INTERESTS WITHOUT UNDULY BURDENING LEGITIMATE COMMERCIAL SPEECH.

82 Having defined the interesrs we aim to protect, we now turn to the means. Commenters have proposed two generalmethods for ensuring that a customer's privare account information is not used or disclosed in a manner that is inconsistent with the customers' expectations or wishes: opt-in and opt-out. Opt-out (implied approval) is shorthand for a method in which companies provide a customer notice of what the company intends to do with information about the customer and the customer is presumed to have assented to the use unless he or she takes some action to revoke that presumed permission. In other words, the cusromer must "opr out" of the company's proposed plan to use or disclose the customer's information.

xi Opt-in (express approval) refers to a method of determining a customer's preference in which rhe company must convince the customer to take some affirmative step to register thar approval of the use proposed by the company.

A. The opt-out method places a lesser burden on companies' use of customer account information, but recent experiences with its use demonstrate that it needs improvement.

84 The companies favor the use of the opt-out method. Qwesr claims that of the two methods, opt-out is the only one that results in a large enough percentage of customer "approval" to justify the expense to the company of even trying *to* obtain such approval for marketing use. We are sympathetic *to* this problem in those circumstances in which it is unlikely that customers would strongly object, and might actually benefit from, the company's proposed use. The

FCC also found this argument compelling with respect to in-company marketing use of CPNI and consequently allowed opt-out for such uses as require any customer approval.

85 A fundamental difficulty to be overcome by opt-out regulations is that the companies responsible for implementing such regulations may have an incentive *not* to provide a notice that customers will actually recognize, take the time to read, understand, and easily register a disapproving response.[45] As a result, previous attempts at making opt-out schemes work have failed to some degree in (1) getting customers' attention,[46] (2) presenting them with their options in language they understand,[47] and (3) providing them with a simple manner of registering their disapproval, if they so choose.[48]

86 In light of comments and information presented by various commenters regarding recent experience under the Gramm-Leach-Bliley Act and our own

---

[45] *Comments of the Electronic Privacy Information Center (EPIC) of May 22, 2002, p. 4-5, 9-11.* However, as the Qwest experience shows, there is also good reason to avoid making customers so upset as to generate significant ill will.

[46] *Comments of EPIC of May 22, 2002, p. 9; Comments of Attorneys General to FCC of December 21, 2001 (attachment to Public Counsel Comments of January 31, 2002), p. 8* (referring to two surveys concerning Gramm-Leach-Bliley Act opt-out notices: American Banker's Association survey which found that 41 percent of customers did not recall receiving their opt-out notices, 22 percent recalled receiving them but did not read them, and only 36 percent reported reading the notice; and Harris Interactive for the Privacy Leadership Initiative survey, which indicated that only 12 percent of consumers carefully read the notices most of the time, whereas 58 percent did not read the notices at all or only glanced at them).

[47] *Comments of Attorneys General, p. 8* (referring to conclusions of readability expert Mark Hochhauser, Ph.D. that Gramm-Leach-Bliley opt-out notices, which are required under the law to be written in a "clear and conspicuous" manner have been unintelligible and couched in language several grade levels above the reading capacity of the majority of Americans).

[48] We note that those telecommunications companies that have sent opt-out notices have registered opt-out totals that are substantially lower than one would expect from polling data concerning Americans' attitudes about privacy. For example Verizon reports that only 2 percent of its customers, nationally, have opted-out. *Comments of Verizon of May 22, 2002.* Sprint reports that only 5.6 percent of its Washington customers have opted-out. *Comments of Sprint of March 26, 2002, p. 9.* By comparison, a survey that Qwest views as favorable to its advocacy for opt-out places the number of "privacy fundamentalists" in the U.S.—who presumably would opt-out of any kind of data sharing if they only knew how—at 24 percent of the population. More dramatically, a January 2002 Rocky Mountain Poll in Arizona revealed that only 3.7 percent of polled adults believed that Qwest was on the right track when it announced it would sell customer records unless customers took the initiative to contact the company and object within a specific period of time. *Comments of Public Counsel of May 22, 2002, p. 14.* The findings of this latter poll are consistent with our own observation of consumer reaction to the Qwest opt-out notice in our state. Similarly, in a statewide referendum in North Dakota in June, 2002, 72 percent of voters favored repealing a 2001 state law that let financial institutions share or sell customer information unless customers opted out. The repeal reinstated previous state law barring such sharing unless customers opted in. *Adam Clymer, North Dakota Tightens Law on Bank Data and Privacy, New York Times, June 13, 2002.*

cxpcriencc with the Qwest opt-out notice, we arc adopting provisions to improve the visibility and content of the notices and to make it easier for customers to register their disapproval.

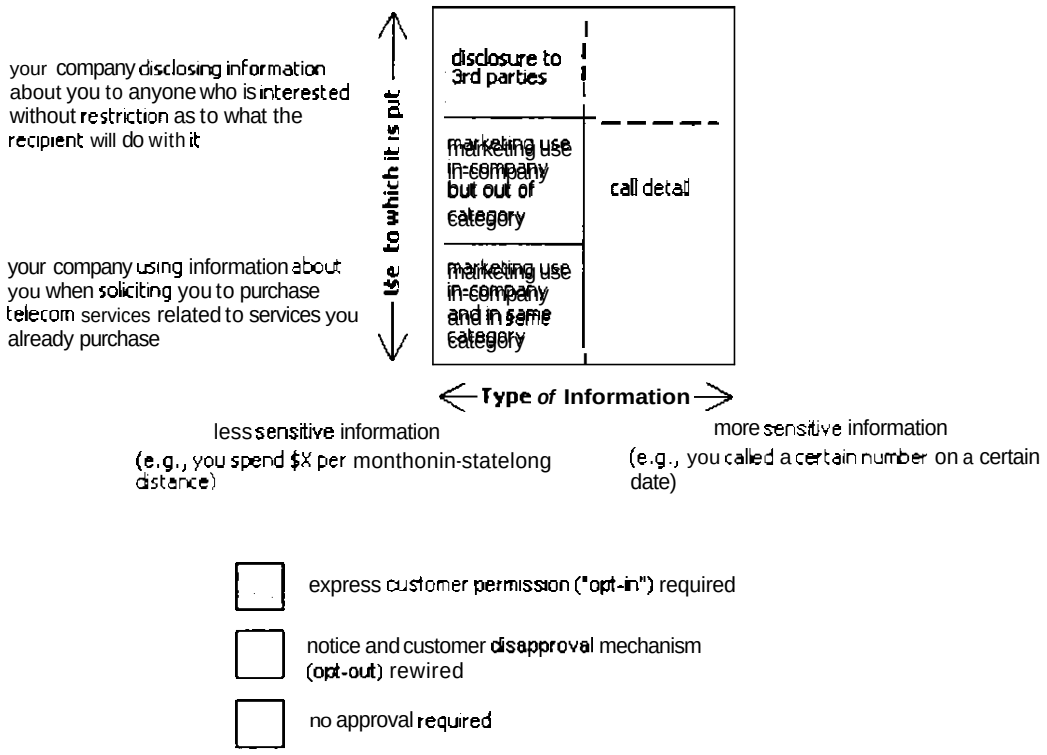
B. Opt-in makes it more difficult for companies to obtain approval, but because it is less likely to result in accidental approval by the customer, it is appropriate for use where customers' privacy expectations are highest.

87 A number of the telecommunications company commcntcrs objected to an opt-in requirement bccausc it puts the burden on the companies to overcome inertia by enticing customers with promises of specific benefits. We have no reason to doubt Qwest's assertion that it likely will not gain customers' opt-in approval in anything approaching the same numbers as through the opt-out method. We accept for argument's sake that many customers who might not actually object to the proposed use will nor take the time to read such a sohcitation and register their approval.

88 We find, however, that an opt-in approach is far less likely to result in the customer's accidental approval of the use of his or her private account information. For this reason, where the potential harm of unauthorized disclosure is most serious and where customers' reasonable expectations of privacy are most solidly rooted in existing law, we find it necessary to require companies to obtain customer's opt-in approval.

XY The schematic in Table 1 may be helpful to illustrate the consequences of our decision regarding where we find opt-in approval is necessary to protect customer's reasonable privacy expectation, where opt-out is sufficient in light of companies' commercial speech interests, and where no approval is necessary.

TABLE 1



90 The whole box, in Table 1, represents the universe of individually identifiable customer proprietary network information and ever). use to wh c h it might be put (aside from delivering service, billing for service, or responding to requirements of other applicable laws). The different degrees of shading in various parts of the box havc the meaning set out in the key **at** the bottom of the illustration.

91 Imagine that the types of information that companies possess about their customers are arrayed on **a** continuum from the left to the right of the box, with the least "private" or sensitive **at** left edge and the most private at the right edge of the box. Next imagine that the types of uses to which the companies might put such information are arrayed on **a** continuum from the bottom to the top of the box. At the very bottom are those uses that are most likely to be within customers' expectations about how a company would use information about them and that are therefore unlikely to upset reasonable privacy expectations. At the cop are those uses that a customer would least expect,

which would therefore be most upsetting to reasonable privacy expectations, and most chilling to the exercise of customers' free speech and association.

92 Unlike the FCC's rules, our rules acknowledge that some types of information are too sensitive or private for any use other than what is necessary to deliver and bill for service. The FCC's rules acknowledge only the dimension (uses of CPNI) that runs from bottom to top. Because of the breadth of the definition of CPNI,[49] we find it imperative to acknowledge the second dimension (i.e., from left to right of the box in Table 1).

93 We discuss our conclusions with respect to each of the shaded areas of this schematic in the sections that follow.

C. We require opt-in for any use of call detail information.

94 Unlike the FCC, we require express, opt-in customer approval before a company may garner information about individual customers' *communications* patterns (as distinct from more generic information about their *purchasing* patterns) except as technologically necessary to provide service and billing. This requirement is represented by the dark-shaded portion on the right side of the box in Table 1. We apply this protection even if the company's sole purpose is to compile information for use in targeted marketing of its own services. To protect customers from this kind of intrusion without their consent we define a category of information known as "call detail." This is the information that commenters universally acknowledge to be the most sensitive or private information that companies possess about their customers.

95 Call detail includes any information about particular telephone calls, including the number from which a call is made, any part of the number to which it was made, when it was made, and for how long. It also includes aggregated information about telephone calls made to or from identifiable individuals or entities, and information about unanswered calls that is specific to a particular period of time. We carve out call detail for special protection because we find that the compilation of usage profiles from this information constitutes a

[49] The definition we adopt for CPNI inserts the words "including call detail" into Congress's definition, which already encompasses call detail. We insert the phrase so our rules are easier to follow where we treat only that subset of CPNI that is call detail—as distinct from "private account information," which makes up the other component of personally identifiable CPNI.